• 量子信息专栏 •

区块链在量子时代的机遇和挑战

颜世露[1]，相里朋[2]，崔 巍[1*]

(1. 华南理工大学自动化科学与工程学院 广州 510640；2. 工业和信息化部电子第五研究所 广州 511300)

【摘要】区块链是随着数字加密货币而逐渐兴起的一种全新的去中心化基础架构。以区块链为底层技术的应用范畴早已超越数字加密货币，延伸到了金融、经济、科技和政治等各个领域。与此同时，具有重大科学意义和战略价值的量子科技正在迅速发展，在即将到来的量子时代，区块链将面临量子科技带来的前所未有的机遇和挑战。主要体现为：一是强大的量子计算对区块链密码体系造成极大威胁，二是在区块链中应用量子科技能有效提高系统的安全性。分析了量子计算攻击区块链的不同方式，指出量子科技赋能区块链的发展现状和趋势。“区块链+量子计算”的交叉融合研究具有重大的现实意义，量子区块链必将成为未来高新技术产业的研究热点。

关 键 词 区块链； 数字加密货币； 量子计算； 量子科技

中图分类号 TN918.91 文献标志码 A doi:10.12178/1001-0548.2021374

Opportunities and Challenges of Blockchain in the Quantum Era

YAN Shilu[1], XIANG Lipeng[2], and CUI Wei[1*]

(1. School of Automation Science and Engineering, South China University of Technology Guangzhou 510640;

2. The Fifth Electronic Research Institute of MIIT Guangzhou 511300)

Abstract Blockchain is a new decentralized infrastructure emerging with digital cryptocurrencies. The application scope of blockchain as the underlying technology has already gone beyond digital cryptocurrencies, extending to various fields such as finance, economy, technology and politics. At the same time, quantum technology with great scientific significance and strategic value is developing rapidly. In the coming quantum era, blockchain will face unprecedented opportunities and challenges brought by quantum technology. It is mainly reflected in the following aspects: firstly, powerful quantum computing poses a great threat to the blockchain cryptosystem; secondly, the application of quantum technology in blockchain can effectively improve the security of the system. This paper mainly analyzes the different ways of quantum computing to attack blockchain in the coming quantum era. We also point out the development status and trend of quantum technology enabling blockchain. "Blockchain + Quantum Computing" cross fusion research has great realistic significance and quantum blockchain will become the focus in the future high-tech industries.

Key words blockchain; digital cryptocurrencies; quantum computing; quantum science and technology

区块链技术最早可追溯到 2008 年发布的关于比特币的白皮书[1]。经过多年发展，以区块链为底层技术的应用已覆盖数字加密货币、金融、经济、科技和政治等领域。2019 年 10 月 24 日，习近平总书记在中央政治局第十八次集体学习时就明确强调了需要加快发展区块链，国内区块链技术也由此进入国家顶层设计之中，区块链产业相继布局。根据“区块链之家”2021 年 10 月 31 日最新监测数据，国内公开区块链项目 2 040 项，区块链相关企业注册数量达到 91 976 家，仅 2020 年新增企业数量就达 26 100 家，创历史新高。同时，全球区块链投融资规模逐年上涨，2020 年全球企业区块链支出规模达到 43 亿美金，占 IT 行业总规模的 0.95%，呈现出巨大的发展潜力[2-3]。

另一方面，诞生于 20 世纪初的量子科技正逐渐成为新一轮科技革命和产业变革的前沿领域。2018 年 12 月，美国国会高票通过《国家量子倡议法案》，并正式颁布了《国家量子计划法》。当

收稿日期：2021－12－23；修回日期：2022－01－29

基金项目：国家自然科学基金 (61873317)

作者简介：颜世露 (1996－)，男，主要从事量子算法方面的研究.

*通信作者：崔巍，E-mail：aucuiwei@scut.edu.cn

前，IBM、谷歌、微软、Rigetti 等美国科技企业在量子计算机物理系统、体系结构、应用软件以及智能算法等研究和应用上处于领先水平。2019 年 9 月 20 日，谷歌公司研究人员架设出名为“悬铃木”的量子计算机，号称能在 3 min 20 s 内解决传统超级计算机可能耗时 1 万年才能处理的问题，实现所谓的“量子霸权”[4]。2020 年 10 月 16 日，中央政治局就量子科技研究和应用前景举行了集体学习，习近平总书记强调，要充分认识推动量子科技发展的重要性和紧迫性，加强量子科技发展战略谋划和系统布局。2021 年 10 月 25 日，中国科学技术大学研究团队的两篇实现“量子计算优越性”的论文同时在国际期刊《物理评论快报》上发表：中国超导量子计算机首次实现量子计算优越性[5]；光量子计算机九章 2.0 相比九章 1.0 实现了更大规模的量子计算优越性[6]。此外，中国的科技企业，如阿里巴巴、腾讯、华为、百度、京东、字节跳动、国盾量子、本源量子等也纷纷布局量子智能计算产业，并取得诸多自主创新成果。

可见，量子科技正在迅猛发展，强大的量子计算能力给基于密码学的区块链系统安全带来了潜在的威胁。根据文献 [7] 的估计，到 2027 年，量子计算机或许能在 10 min 内 (比特币系统生成一个新区块的时间) 打破基于椭圆曲线密码的数字签名方案，对比特币系统造成毁灭性的破坏。同时，量子科技如量子密钥分发、量子秘密共享、量子身份认证、量子数字签名以及量子随机数等基于量子力学的应用可为区块链提供无条件安全保障。可见，量子科技在给区块链技术带来巨大挑战的同时也带来了极大的革新机遇。

为此，本文针对量子科技给区块链带来的挑战和机遇研究现状进行了总结，并指出“区块链+量子计算”交叉融合研究已经成为不可阻挡的发展潮流，具有重要的现实意义。

1　区块链系统技术体系

区块链是分布式存储、点对点传输、共识机制、加密算法、智能合约等多种计算机技术的新型应用模式，是多种技术有机结合的技术集成体系[8]。一般而言，区块链系统可分为数据层、网络层、共识层、激励层、合约层和应用层。数据层封装了底层数据区块以及对应的数据加密技术；网络层包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装各类共识算法；激励层将经济因素集成到区块链技术体系中，包括经济激励的发行和分配机制等；合约层主要封装不同用途的各类算法和智能合约，以实现区块链可编程特性和可扩展性[9-11]。

从应用视角来看，区块链可被理解为通过共识协议保证节点间账本数据一致，通过密码学保证交易数据不可篡改与发送安全的点对点 (集体维护、去中心化) 的分布式数据库。所有网络节点是平等的关系，都可以访问、监督和使用该数据库。用户节点之间产生数据信息，将数据信息进行全网广播，接收节点将数据信息打包至新区块中，网络节点执行共识算法，并将验证结果进行全网广播，通过全网络节点的共识验证后，将该数据区块加入区块链中。因为区块链系统节点较多、分布较广，且不同节点之间的通信存在延迟，需要共识机制 (分布式共识算法) 决定新区块的记账权以保证节点数据的一致性。共识机制设计极大地影响区块链系统的性能，包括交易能力、可扩展性和分区容错能力。在分布式系统学科上，分布式节点如何在不可信的网络环境中达成一致性和可用性一直是需要解决的难题。针对此问题，根据实际应用场景，目前已经产生许多代表性成果：如以工作量证明机制 (proof of work, PoW) 为代表的证明类共识协议[1]、以实用拜占庭容错协议 (practical Byzantine fault tolerance, PBFT) 为代表的拜占庭类共识协议[12] 和以 Raft 为代表的传统分布式一致性算法[13]。

加密算法是区块链系统安全性保障的基础，其中使用到的密码技术主要包括哈希算法、公钥密码技术、数字签名、零知识证明等。哈希算法能保护账本数据免受未授权的修改，具有检测区块是否被篡改的能力，是实现区块数据完整性保护的主要工具。不同于传统的对称密码算法，公钥密码采用了两个相互关联的秘钥，分别是需要公开的公钥和需要保密的私钥。公钥密码体系的提出，有效地应用数字证书解决了秘钥分发的问题，并进一步提出了有效的数字签名以确保区块链数字资产确权的安全性。

2　量子计算对区块链系统的攻击范式

量子计算机具有远超于经典计算机的强大计算能力，因而对区块链系统产生巨大威胁，严重危及区块链产业的发展。文献 [7, 14-15] 将量子计算攻击区块链系统的方式总结为两种：一是 Grover 算法对哈希算法的攻击；二是 Shor 算法对公钥密码的攻击。

2.1 Grover 算法对哈希算法的攻击

哈希算法是一种能将任意长度的输入值映射为较短的固定长度的二进制值的算法，其具有以下特性：1) 确定性：给定一个输入值，其输出值是唯一且确定的；2) 单向性：给定一个输入值，很容易计算出其哈希值，但是给定哈希值，根据同样的算法难以计算得到原输入值；3) 抗碰撞性：要找到相同输出的两个不同输入值，在计算上几乎是不可能的；4) 雪崩效应：当输入值发生极其微小的改变时，也会导致输出的完全不可区分性的改变。因为这些特性，哈希算法常常被用于检验数据的完整性、快速查找和对数据进行加密，其在区块链中也有着广泛的应用。如比特币中的 Merkle 树 (如图 1) 中的所有节点信息都是应用 SHA-256 哈希运算得到；以太坊账户地址是应用 Kec-cak-256 哈希运算一个公钥得到；而比特币地址，则是通过对一个公钥进行 SHA-256 和 RIPEMD160 哈希运算得到；区块链中使用的数字签名是对经过哈希运算后的消息进行签名的。

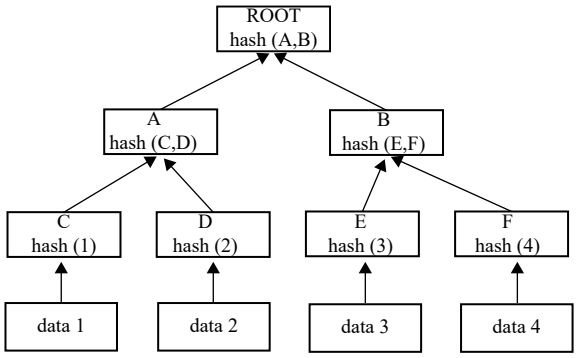

图 1 Merkle 树结构图

对于非结构化数据库，经典的暴力搜索算法复杂度随着输入变量的增长而呈线性增长，而量子科技中的 Grover 算法利用量子叠加的性质以及迭代过程，实现了对无序数据库搜寻问题的二次加速[16]。理论上，应用了哈希算法的区块链技术都面临着 Grover 算法的威胁，相对于经典计算机，其安全性降低到原来的开平方级别[7]。下面以比特币系统中的工作量证明机制为例，说明 Grover 算法对区块链共识机制的影响。PoW 机制是一个具有开创性的共识算法，其将经济激励与共识过程相融合，通过奖励保持节点持续挖矿，以及通过极高的攻击难度和成本保持节点诚实守信，从而增强了网络的可靠性与安全性。基于哈希算法的 PoW 机制主要利用了哈希算法的特性，使网络中各个节点利用自身的计算资源寻找特定前缀的哈希值以竞争区块的记账权。首先矿工节点生成区块奖励 coinbase 交易，并将其和从交易池中选取的普通交易组成如图 1 所示的 Merkle 树；接着把 Merkle 树根节点 (ROOT) 的哈希值、时间戳、目标值、随机数、上一个区块头哈希值和版本号等信息组成 80 个字节的区块头；最后将这个区块头作为工作量证明的输入，对整个区块头进行两次 SHA-256 哈希运算。运算结果与当前比特币网络中的目标值进行比较，如果小于目标值，并在广播后得到全网多数矿工的认可，则挖矿成功，否则修改随机数继续运算。由于哈希算法的单向性和雪崩效应等特性，寻找符合条件的区块成为暴力穷举问题。Grover 算法通过加速对逆哈希问题的暴力穷举 (加速穷举随机数)，能更快找到符合条件的区块，进而通过以下两种方式攻击比特币系统：一是通过加速哈希碰撞来伪造区块，以篡改覆盖原来区块中的所有交易信息 (如图 2a)；二是造成 51% 的算力攻击 (如图 2b)。通过快速挖矿来获得比特币奖励，同时主导新区块的生成。甚至在非常短的时间内重建一条新的分支链，当分支链的长度超过主链时，分支链就可以取代主链，从而导致原来的主链记录完全被覆盖。具体而言，攻击者可以阻止新交易的确认，和撤销在网络被控制时完成的交易，从而实现双重花费。无论哪种攻击，都是从本质上破坏了比特币系统的公信力，使得比特币失去本身的价值。

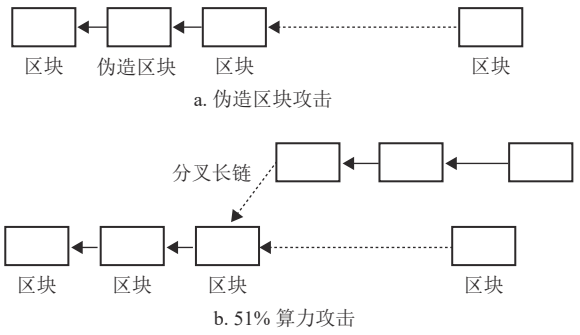

图 2 Grover 算法对比特币系统的两种攻击方式

2.2 Shor 算法对公钥密码的攻击

公钥密码是基于数学难题而非基于传统的替换和置换算法，因而具有更高的安全性。区块链系统中存在着大量公钥密码的应用，如数字签名、资产确权、身份认证等，其数学原理主要包括：离散对数难题 (discrete logarithm problem, DLP)、大整数分解难题 (integer factorization problem, IFP) 和椭圆

曲线离散对数难题 (elliptic curve discrete logarithm problem, ECDLP) 等。对于 IFP 和 ECDLP，传统算法中最有效的方法是由文献 [17] 提出的通用数域筛选算法 (general number field sieve, GNFS)，但该方法的时间复杂度仍然是亚指数的。当非对称密码中基于 IFP 的 RSA 密码需要分解的整数 n 非常大时，经典认知中 RSA 密码是安全的。但在理论上，量子科技中的 Shor 算法依据数论中的相关定理，可将大数因子分解转化为求函数周期问题，能够指数级提高大整数的质因子分解速度，从而对公钥密码造成毁灭性的攻击。物理学家们一直致力于量子计算机的仿真实现[18-25]。最新研究表明：使用 13 436 个物理量子比特和一个存储时间为 2 h 的多模存储器制成的处理器，可能在 177 天内完成对 2 048 位 RSA 整数的分解[25]。另外，基于量子退火原理的 RSA 破译是一种新的量子计算攻击公钥密码的算法，与 Shor 算法原理上有本质不同，其将破译 RSA 问题转换为组合优化问题，利用量子退火算法独特的量子隧穿效应跳出局部最优解逼近全局最优解，和经典攻击算法相比依然具有指数级加速的潜力[26-29]。一旦通用量子计算机可以被造出来，通过暴露在区块链中的公钥，黑客可以运行 Shor 算法求解 ECDLP，从而计算出私钥，实现对数字资产的转移。

3　量子科技赋能区块链

面对强大的量子计算对区块链造成的威胁，目前急需更加安全的理论以保证区块链产业的发展，而量子科技具备的经典不可比拟的量子特性可以为区块链提供安全保障。当前区块链系统被量子计算攻破的原因主要还是对哈希算法和公钥密码体系的攻击，在比特币系统中体现为对 PoW 共识机制和数字签名技术的攻击。因而，量子技术赋能区块链系统的主要思路为：构建一个基于非哈希计算的共识机制和基于非公钥密码的安全保障体系。目前一般有两种实现方式：1) 后量子区块链，将后量子签名算法代替经典签名算法。但此方案是基于目前某些不能被量子计算机有效解决的计算复杂性困难问题，并不能提供无条件安全证明。2) 量子区块链，即以量子物理特性为基础，在 P2P 网络中应用量子通信技术，在区块链系统中应用量子拜占庭共识算法、量子数字签名、量子随机数等，使得区块链系统更加安全，以对抗目前已知的量子计算攻击。下面主要针对第二种方式展开阐述。

3.1　量子通信

量子通信是利用微观粒子的量子态以及量子纠缠效应进行信息传递的一种新型通信方式，近年来逐渐从理论走向实验和实用化发展。量子通信过程中如果出现任何攻击拦截行为，都会导致信息传递载体——量子态发生变化，通信双方能轻易发现攻击行为，从而终止通信。这样一来，任何攻击方式都无法得到量子态上所传递的原有信息，信息泄露等问题不会发生。“一次一密”(one-time pad, OTP) 加密技术已被证明能够保障通信过程中信息的绝对安全。

当前的量子通信技术主要分为量子密钥分发 (quantum key distribution, QKD) 和量子隐形传态 (quantum teleportation, QT) 两类。自 1995 年中科院物理所实现国内首次 QKD 开始，到 2004 年京−津现网实验，逐步展开了试点应用。自 2017 年始，“沪杭干线”“宁苏干线”“武合干线”等项目开始建设，迄今已取得不错的成绩。行业内部分企业已经具备量子通信设备的研发生产能力，如国盾量子、问天量子等，这些企业也推动了量子通信行业的持续发展。QT 技术也逐渐从实验室走向应用。2005 年中科大首次实现国内 13 km 的 QT 传输，2020 年 6 月，《自然》杂志在线发表了题为“基于纠缠的千公里级安全量子加密”的研究论文[30]，意味着我国迈开了构建全球化量子密钥分发网络甚至量子互联网的重要一步。

量子通信技术的发展虽然历时较短，但其发展态势迅猛，表现出巨大的潜力。在区块链系统中应用量子通信，有望达到无条件安全、高效抗干扰等效果。量子智能算法、量子拜占庭共识算法、量子随机数等量子互联网上层应用都直接依赖于量子通信，其安全性由量子力学基本原理给予保障。

3.2　量子拜占庭共识算法

影响共识机制安全性的最重要问题就是解决各节点如何在不可信的网络环境中达成一致的难题。该难题的解决方法和文献 [31] 提出的拜占庭将军问题异曲同工：在已知有将军是叛徒的情况下，其余忠诚的将军如何达成一致协议。目前区块链中应用的共识算法，如 PoW、PBFT 等，都是结合实际的应用场景，从一定程度上给出了拜占庭将军问题的可行解。

实际上，理论早已证明：在没有共享任何初始信息的前提条件下，如果有超过 1/3 的将军是叛军，则拜占庭将军问题无解。但可检测的拜占庭协

议将拜占庭将军问题转化为秘密数字列表的生成和安全分发问题，便可能从根本上解决问题。经典的分发方案的安全性依赖于哈希算法和公钥密码，对于具有超越经典的量子计算而言，公钥密码体系理论上可以在极短的时间内被破解，就意味着没有安全的秘密列表可用。量子通信技术结合量子计算可以无条件安全分发秘密数字列表，实现可检测的拜占庭共识协议[32-40]。另一方面，可从 GHZ 态的量子纠缠的角度实现 N 个节点对数据的共识：

1) 制备 N 个量子比特的 GHZ 态；

$$\mathrm{GHZ}=\frac{|0\rangle^{\otimes N}+|1\rangle^{\otimes N}}{\sqrt{2}}$$

2) 对于 N 个节点的区块链系统，将 GHZ 态的每个比特分发给系统中的每个节点；

3) 每个节点测量自己的量子比特；

4) 测量结果为$|0\rangle$则共识 0，否则共识 1；

这样，对于存在 3 个网络节点的区块链系统，即使存在一个以上的恶意节点，也能通过量子拜占庭共识协议保证区块链中所有诚实节点达成一致的行为。量子科技提高了分布式系统中可承受恶意节点的阈值，进而提高区块链系统的安全性。

3.3 量子数字签名

数字签名由于可以提供消息认证、确保消息的完整性及实用性而得到了迅速推广。但经典数字签名的安全性是基于数学难题的计算复杂性的，没有严格的安全保障，因此密码学家们开始研究不同于经典的数字签名。自文献 [41] 利用量子态的纠缠性提出了第一个量子签名协议后，许多量子数字签名方案被相继提出，包括基于 GHZ 三重态的相干性和量子密钥分发协议的仲裁量子签名方案[42]、基于量子一次一密和 GHZ 三重态的相干性的量子签名方案[43]、基于量子隐形传态的群签名方案[44-45]、量子代理签名[46] 及量子盲签名[47] 等。

量子数字签名的应用主要分为密钥分发阶段和签名验证阶段。各节点间密钥分发阶段的安全性由量子密钥传输保障，签名验证阶段需要结合量子特性和具体协议完成设计。基于量子力学基本原理的量子数字签名能达到无条件安全的信息交互的效果。各种面向不同应用场景的量子数字签名能从原理上抵抗算力攻击，增强区块链系统的资产认证和确权的安全性。

3.4 量子随机数

随机数在计算机系统、信息安全等领域有着重要应用。目前常用的随机数主要是依靠计算机产生的伪随机数，或者是从某些经典物理噪声 (如电噪声等) 中提取出来的随机数，其在考虑到所有变量的情况下可被模拟，存在着极大威胁。区块链系统中随机数的使用随处可见，如商用分布式设计区块链操作系统 (enterprise operation system, EOS) 中的博彩游戏身份验证，共识算法如 PBFT 等的主节点随机选举，这些过程的随机性要能得到全网的确认，是不能被操控和不能被预测的，否则恶意攻击者通过操控这个随机数就可以操控长链、转移代币，对区块链的公信力和安全性造成破坏。

量子不可测量原理能够实现具有不可预测性、不可重复性和无偏性等特征的无条件安全的量子随机数。经多年研究，量子随机数发生器的实现和应用也得到了充分发展[48-50]。量子随机数发生器可被分为实用化的量子随机数发生器、自检测量子随机数发生器及半自检测量子随机数发生器[51]。不同的量子随机器存在着不同的各有优势的应用场景。中国科学技术大学联合浙江大学通过研制硅基光子集成芯片和优化实时后处理，实现了迄今最快的速率达 18.8 Gbps 的实时量子随机数发生器[52]，为开发商用量子随机数发生器奠定了技术基础。可以预见，量子随机数发生器最有可能在近期应用于区块链系统，增强系统的安全性和稳定性。

3.5 量子区块链

目前已有不少学者尝试探索研究独立完整的量子区块链系统。文献 [53] 以经典区块链结构为基础，引入了公钥量子货币与泛化通用组合 (generalized universal composability, GUC) 框架，并将经典智能合约与量子闪电[54] 相结合，提出了经典–量子混合支付区块链系统。文献 [55] 提出一种新型量子区块链，其将区块信息编码成一连串彼此缠绕的光子，这些区块通过时间上的纠缠按时间顺序连接起来，运用量子密钥分发技术代替非对称加密传输，以量子签名进行身份验证，保证任意节点之间数据传输的真实及防篡改。文献 [56] 基于量子纠缠和权益证明机制设计了一个新的量子区块链方案，能抵抗双花攻击、中间人攻击和状态估计攻击，缩短达成交易的时间和减少能源的消耗。但这些方案中涉及的量子技术大多处于理论研究阶段，实现难度大，可行性小。

为此，文献 [57] 提出量子安全区块链解决方案 (quantum-secured blockchain, QB)，在量子网络

层使用 QKD 方式进行对称密钥分发，共识机制采用经典的基于原始状态机复制的拜占庭容错算法。该量子区块链系统已经通过光纤网络进行测试，但系统内通信复杂度较高，不具备可扩展性。文献 [58] 以 QB 区块链框架为基础，提出一种新的量子安全区块链方案 LC(logicontract)，其中采用基于 QKD 的无条件安全 Toeplitz 群签名作为系统的数字签名方案，增加了系统的安全性，但相对于其他哈希函数，Toeplitz 的运算速度较慢且需要占用较大存储空间。另外，LC 区块链只提到采用一种具备抗碰撞性的哈希函数以用于计算哈希指针，所以该方案仍然面临被量子计算攻击的风险，且采用简化后的 YAC(yet another consensus) 共识机制，其容错能力低于主流的拜占庭容错共识机制，也存在着较大的局限性。

4　结 束 语

区块链是新一代信息技术的重要组成部分，已经在防伪溯源、供应链管理、司法存证、政务数据共享及民生服务等领域得到广泛应用。但区块链的基础理论和技术研究仍处于初级阶段，许多涉及底层技术原理的重要科学问题亟待跟进。尤其是在即将到来的量子时代，区块链系统中的数字签名和共识机制[59] 等重要基础技术面临着量子科技所带来的挑战和机遇。目前量子科技的发展还处于 NISQ (noisy intermediate-scale quantum) 阶段[60]，很多工作仍然处于实验室阶段，量子硬件在向 50～100 量子比特发展中还面临着如何保持高相干性、扩展校准技术、提高量子比特连接性、提升门保真度等诸多问题。此外，量子科技的产业化不仅包括量子计算的硬件，还涉及如适应量子计算机架构的基础软件、应用软件、NISQ 设备适用的经典−量子算法和相关服务[61-62] 等内容。

本文梳理了区块链的技术体系，分析了量子科技对区块链的攻击和防御，指出“区块链+量子计算”交叉融合研究已经成为不可阻挡的发展潮流，具有重要现实意义。在未来的量子时代中，区块链将面临前所未有的机遇与挑战：量子计算对区块链的攻击主要集中于量子算法对密码体系的攻击，如哈希算法和公钥密码算法；量子科技赋能区块链能够为未来繁荣的区块链产业提供更安全的保障体系，主要体现在为量子共识机制、量子数字签名、量子随机数等提供潜在的无条件系统安全保障。随着量子通信等技术的逐渐推广，未来的量子区块链必将成为高新技术产业的研究热点，从而得到更加长远的发展。

参　考　文　献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008, 31: 21260.

[2] 中国信通院. 区块链白皮书 [EB/OL]. (2020-12-22). http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201230759713827891.pdf.
China Academy of Information and Communications Technology. Blockchain white paper[EB/OL]. (2020-12-22). http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201230759713827891.pdf.

[3] 火币研究院. 全球区块链产业全景与趋势 2020-2021 年度报告 [EB/OL]. [2021-02-07] https://research.huobi.cn/detail/389.
Huobi Research Institute. Global blockchain industry panorama and trends 2020-2021 annual report [EB/OL]. [2021-02-07] https://research.huobi.cn/detail/389.

[4] ARUTE F, ARYA K, BABBUSH R, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574(7779): 505-510.

[5] ZHONG H S, DENG Y H, QIN J, et al. Phase-Programmable Gaussian boson sampling using stimulated squeezed light[J]. Physical Review Letters, 2021, 127(18): 180502.

[6] WU Y L, BAO W S, CAO S R, et al. Strong quantum computational advantage using a superconducting quantum processor[J]. Physical Review Letters, 2021, 127(18): 180501.

[7] AGGARWAL D, BRENNEN G K, LEE T, et al. Quantum attacks on bitcoin, and how to protect against them[EB/OL]. (2017-10-28). http://arxiv.org/abs/1704.02553.

[8] 邹均, 余斌, 庄鹏, 等. 区块链核心技术与应用[M]. 北京: 机械工业出版社, 2018.
ZHOU J, YU B, ZHUANG P, et al. Blockchain: Core technology and application[M]. Beijing: China Machine Press, 2018.

[9] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: The state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[10] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: Architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[11] 蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术[J]. 计算机学报, 2021, 44(1): 84-131.
CAI X Q, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131.

[12] CASTRO M, LISKOV B. Practical Byzantine fault

tolerance[C]//Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans, LA: [s.n.], 1999: 173-186.
[13] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//Proceedings of 2014 USENIX Annual Technical Conference. Philadephia: [s.n.], 2014: 305-319.
[14] FEDOROV A K, KIKTENKO E O, LVOVSKY A I. Quantum computers put blockchain security at risk[J]. Nature, 2018, 563(7732): 465-467.
[15] CUI W, DOU T, YAN S L. Threats and opportunities: Blockchain meets quantum computation[C]//2020 39th Chinese Control Conference (CCC). Shenyang: IEEE, 2020: 5822-5824.
[16] GROVER L K. Quantum mechanics helps in searching for a needle in a haystack[J]. Physical Review Letters, 1997, 79(2): 325-328.
[17] LENSTRA A K, HENDRIK J W. The number field sieve[C]//The Development of the Number Field Sieve. Berlin: Springer, 1993: 11-42.
[18] VANDERSYPEN L M K, STEFFEN M, BREYTA G. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance[J]. Nature, 2001, 414(6866): 883-887.
[19] LU C Y, BROWNE D E, YANG T. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits[J]. Physical Review Letters, 2007, 99(25): 1-4.
[20] LUCERO E, BARENDS R, CHEN Y. Computing prime factors with a josephson phase qubit quantum processor[J]. Nature Physics, 2012, 8(10): 719-723.
[21] SMOLIN J A, SMITH G, VARGO A. Oversimplifying quantum factoring[J]. Nature, 2013, 499(7457): 163-165.
[22] MONZ T, NIGG D, MARTINEZ E A, et al. Realization of a scalable shor algorithm[J]. Science, 2016, 351(6277): 1068-1070.
[23] GIDNEY C, EKERÅ M. How to factor 2 048 bit RSA integers in 8 hours using 20 million noisy qubits[J]. Quantum, 2021, 5: 433.
[24] EKERÅ M, HÅSTAD J. Quantum algorithms for computing short discrete logarithms and factoring RSA integers[C]//International Workshop on Post-Quantum Cryptography. Cham: Springer, 2017: 347-363.
[25] GOUZIEN E, SANGOUARD N. Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory[J]. Physical Review Letters. 2021, 127(14): 140503.
[26] JIANG S, BRITT K A, MCCASKEY A J, et al. Quantum annealing for prime factorization[J]. Scientific Reports, 2018, 8(1): 1-9.
[27] PENG W C, WANG B N, HU F, et al. Factoring larger integers with fewer qubits via quantum annealing with optimized parameters[J]. Science China Physics, Mechanics & Astronomy, 2019, 62(6): 60311.
[28] WANG X M. Quest towards "factoring larger integers with commercial D-Wave quantum annealing machines" [J]. Science China Physics, Mechanics & Astronomy, 2019, 62(6): 960331.
[29] WARREN R H. Factoring on a quantum annealing computer[J]. Quantum Information & Computation, 2019, 19(3-4): 252-261.
[30] YIN J, LI Y H, LIAO S K, et al. Entanglement-based secure quantum cryptography over 1120 kilometres[J]. Nature, 2020, 582(7813): 501-505.
[31] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem[J]. ACM Transaction on Programming Language and System, 1982, 4(3): 382-401.
[32] FITZI M, GISIN N, MAURER U. Quantum solution to the Byzantine agreement problem[J]. Physical Review Letters, 2001, 87(21): 217901.
[33] GAO F, GUO F Z, WEN Q Y, et al. Comment on experimental demonstration of a quantum protocol for Byzantine agreement and liar detection[J]. Phys Rev Lett, 2008, 101(20): 208901.
[34] GAERTNER S, BOURENNANE M, KURTSIEFER C, et al. Experimental demonstration of a quantum protocol for Byzantine agreement and liar detection[J]. Physical Review Letters, 2008, 100(7): 67-75.
[35] GAERTNER S, BOURENNANE M, KURTSIEFER C, et al. Addendum to experimental demonstration of a quantum protocol for Byzantine agreement and liar detection[EB/OL]. (2008-11-16). http://arxiv.org/abs/0810.3832.
[36] CABELLO A. Solving the liar detection problem using the four-qubit singlet state[J]. Physical Review A, 2003: 68(1): 012304.
[37] RAHAMAN R, WIEŚNIAK M, ŻUKOWSKI M. Quantum Byzantine agreement via Hardy correlations and entanglement swapping[J]. Physical Review A, 2015, 92 (4): 042302.
[38] IBLISDIR S, GISIN N. Byzantine agreement with two quantum-key-distribution setups[J]. Physical Review A, 2004, 70(3): 034306.
[39] BOURENNANE M, CABELLO A, ZUKOWSKI M. Quantum Byzantine agreement with a single qutrit[EB/OL]. (2010-01-12). http://arxiv.org/abs/1001.1947.
[40] TAVAKOLI A, CABELLO A, ŻUKOWSKI M, et al. Quantum clock synchronization with a single qudit[J]. Scientific Reports, 2015, 5(1): 1-4.
[41] 曾贵华, 马文平, 王新梅, 等. 基于量子密码的签名方案[J]. 电子学报, 2001, 29(8): 1098-1100.
ZENG G H, MA W P, WANG X M, et al. Signature scheme based OR quantum cryptography[J]. Acta Electronica Sinica, 2001, 29(8): 1098-1100.
[42] ZENG G, KEITEL C H. Arbitrated quantum-signature scheme[J]. Physical Review A, 2002, 65(4): 042312.
[43] LYU X, FENG D G. An arbitrated quantum message signature scheme[M]//Computational and Information Science. Berlin, Heidelberg: Springer, 2004: 1054-1060.
[44] ZHANG K, SONG T, ZUO H, et al. A secure quantum group signature scheme based on Bell states[J]. Physica Scripta, 2013, 87(4): 045012.
[45] XU R, HUANG L, YANG W, et al. Quantum group blind

signature scheme without entanglement[J]. Optics Communications, 2011, 284(14): 3654-3658.
[46] WEN X, CHEN Y, FANG J. An inter-bank E-payment protocol based on quantum proxy blind signature[J]. Quantum Information Processing, 2013, 12(1): 549-558.
[47] KHODAMBASHI S, ZAKEROLHOSSEINI A. A sessional blind signature based on quantum cryptography[J]. Quantum Information Processing, 2014, 13(1): 121-130.
[48] MA X, YUAN X, CAO Z, et al. Quantum random number generation[J]. NPJ Quantum Information, 2016, 2(1): 1-9.
[49] HERRERO-COLLANTES M, GARCIA-ESCARTIN J C. Quantum random number generators[J]. Reviews of Modern Physics, 2017, 89(1): 015004.
[50] CAO Z, ZHOU H, YUAN X, et al. Source-independent quantum random number generation[J]. Physical Review X, 2016, 6(1): 011020.
[51] 周泓伊, 曾培. 量子随机数发生器[J]. 信息安全研究, 2017, 3(1): 23-35.
ZHOU H Y, ZENG B. Quantum random number generation[J]. Journal of Information Security Research. 2017, 3(1): 23-35.
[52] BAI B, HUANG J, QIAO G R, et al. 18.8 Gbps real-time quantum random number generator with a photonic integrated chip[J]. Appl Phys Lett, 2021, 118: 264001.
[53] COLADANGELO A, SATTATH O. A quantum money solution to the blockchain scalability problem[J]. Quantum, 2020, 4: 297.
[54] ZHANDRY M. Quantum lightning never strikes the same state twice[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2019: 408-438.
[55] DEL R, MATT V. Quantum blockchain using entanglement in time[J]. Quantum Reports, 2019, 1(1): 3-11.
[56] GAO Y L, CHEN X B, XU G, et al. A novel quantum blockchain scheme base on quantum entanglement and DPoS[J]. Quantum Information Processing, 2020, 19(12): 1-15.
[57] KIKTENKO E O, POZHAR N O, ANUFRIEV M N, et al. Quantum-secured blockchain[J]. Quantum Science and Technology. 2018, 3(3): 035004.
[58] SUN X, SOPEK M, WANG Q, et al. Towards quantum-secured permissioned blockchain: Signature, consensus, and logic[J]. Entropy, 2019, 21(9): 887.
[59] AI Z D, CUI W. A proof-of transactions blockchain consensus protocol for large-scale IoT[EB/OL]. (2021-08-30). http://ieeexplore.ieee.org/abstract/document/9524744.
[60] PRESKILL J. Quantum computing in the NISQ era and beyond[J]. Quantum, 2018, 2: 79.
[61] DOU T, ZHANG G F, CUI W. Efficient quantum feature extraction for CNN-based learning[EB/OL]. (2022-01-07). https://arxiv.org/abs/2201.01246.
[62] YAN S L, DOU T, SHU R Q, et al. Module for arbitrary controlled rotation in gate-based quantum algorithm [EB/OL]. (2021-07-17). https://arxiv.org/abs/2107.08168.

编　辑　蒋　晓